

ANTI-MONEY LAUNDERING & COUNTERING THE FINANCING OF TERRORISM POLICY

1. PURPOSE

This Policy aims to provide and formalize guidelines, rules and procedures to guide the Company in preventing and combating money laundering and the financing of terrorism.

2. FIELD OF APPLICATION

The contents of this Policy shall be observed by all employees, partners, suppliers and service providers, in addition to any player in the Company's value chain.

3. DEFINITIONS

- **Client:** individuals or companies which purchase products or use the services provided by americanas s.a.
- **COAF (Brazilian Financial Control Council):** agency created within the scope of the Ministry of Finance with the purpose of governing, applying administrative penalties, receiving, examining and identifying suspected occurrences of illegal activities provided for in Law No. 9.613/1998, without prejudice to the powers of other agencies and entities.
- **Company:** comprises americanas s.a. and all other related companies as direct and indirect, current and future subsidiaries.
- **Financing of Terrorism:** consists of allocating funds to individuals and/or organizations having the intention of promoting intended or calculated criminal acts with the aim of provoking a state of terror in society.
- **Money Laundering:** consists of a set of commercial or financial transactions aiming to place illegal proceeds into the financial system, concealing their sources and, accordingly, giving them a legitimate appearance.
- **OFAC (Office of Foreign Assets Control) List:** List issued and updated on a regular basis by the U.S. Treasury, containing names and associations of individuals and companies restricted due to connection with wrongful acts, such as drug trafficking, money laundering, terrorism, among others.
- **Partner(s):** individuals or companies with business relationships with the Company.
- **PEP (Politically Exposed Persons):** PEPs are considered to be individuals who, in the last 5 (five) years, fall into the following categories: i) holders of elective offices of the Executive and Legislative Branches of the Federal Government; ii) holders of positions, in the Executive

Branch, of Minister of State or equivalent, Special Nature or equivalent; iii) president, vice-president and director, or equivalent, of entities indirectly controlled by the government; iv) holders of positions, in the Executive Branch, of the Group of Higher Management and Advice – DAS, level 6, or equivalent; v) members of the National Council of Justice, the Supreme Federal Court, the Superior Courts and the Federal Regional, Labor and Electoral Courts, the Superior Council of Labor Justice and the Federal Justice Council; vi) members of the National Council of the Prosecutor's Office, the Federal Attorney General, the Vice-Federal Attorney General, the Attorney General of Labor, the Attorney General of Military Justice, the Deputy Federal Attorneys General and the Attorneys-General of the States and the Federal District; vii) the members of the Federal Accounting Court and the Attorney General of the Prosecutor's Office at the Federal Accounting Court; viii) national chairmen and treasurers, or equivalent, of political parties; ix) the governors and secretaries of the States and the Federal District, the State and District Deputies, the chairmen, or equivalent, of entities indirectly controlled by the States and the Federal District and the chairmen of Courts of Justice, of Military, of Accounts or equivalent of the States and the Federal District; x) Mayors, City Councilors, Chairmen of Accounting Courts or equivalents of Municipalities and Chairmen of Municipal Chambers of State capitals. Individuals who, abroad, are also considered PEPs: i) heads of state or government; ii) senior politicians; iii) holders of government positions at higher levels; iv) general officers and members of higher echelons of the judiciary, the legislative or the military branches; v) senior executives of public corporations; vi) leaders of political parties; or vii) senior managers of entities governed by public or private international law.

4. GUIDELINES

The Company:

- Does not tolerate the practice of any activity with the aim of simulating or concealing proceeds (money laundering) and terrorist financing.
- Exercises the parameters defined in Law No. 9.613/98 to prevent and combat money laundering and terrorist financing activities.
- Adopts a risk-based approach by establishing procedures to review, identify, understand and mitigate the risk of its activities and services being involved in money laundering and terrorist financing.
- Adopts procedures in the development of products or services to assess the risk of their use in money laundering and terrorist financing practices.

- Establishes, if necessary, preventive mechanisms that are flexible and proportional to the nature of the risks to which it is exposed, with a focus on preventing money laundering and the financing of terrorism.
- Monitors all transactions or proposed transactions in order to identify cases considered to be evidence of money laundering or financing of terrorism.
- Evaluates, in suspicious transactions, the form of payment used, the frequency, the parties and amounts involved, the capacity and economic activity of those involved and any other additional evidence of wrongdoing or illegality involving the parties and their transactions.
- Notifies the competent authorities of transactions or proposed transactions that have been identified as evidence of money laundering or financing of terrorism, in accordance with applicable law.
- Assigns a confidential label to any information related to reports, evidence, or suspected involvement with acts related to money laundering and financing of terrorism.
- Adopts Know Your Customer procedures to accurately identify key information about its customers and, accordingly, classify each one according to the degree of risk they pose to the Company in relation to money laundering and financing of terrorism.
- Establishes criteria for recruiting and hiring new employees and adopts Know Your Employee procedures to monitor employees' conduct that may pose any type of risk or deviation.
- Adopts Know Your Partner procedures in order to prevent the establishment and maintenance of relationships with untrustworthy partners or those suspected of involvement in money laundering and terrorist financing activities.
- Adopts Know Your Supplier procedures to identify and accept suppliers and service providers in order to prevent the engagement of disreputable companies or companies suspected of being involved in money laundering and terrorist financing activities.
- Adopts procedures to identify and monitor customers, partners, suppliers and service providers that may be on PEP, OFAC, or other restrictive lists.
- Reports any customers, partners, suppliers and service providers listed in the OFAC list to the competent authority.
- Establishes restrictive measures regarding the conduct of business and the maintenance of relationships with customers, partners, suppliers and service providers when circumstances imply evidence of involvement in money laundering and terrorist financing practices.

- Disseminates the procedures adopted to inhibit the practice of money laundering and terrorist financing offenses and provides a training program for its employees on the subject.
- Reviews, at least on an annual basis, the guidelines defined in this Policy.
- Evaluates from time to time compliance with and effectiveness of this Policy, procedures and internal controls in terms of preventing and countering money laundering and financing of terrorism.

5. WHISTLEBLOWER CHANNEL

The Company provides a whistleblower channel for employees, customers, partners, suppliers, service providers, or any third-parties who identify any violations to the guidelines under this Policy or conduct suspected of involvement with money laundering and terrorist financing offenses.

The report must be made via website at <http://canaldedenuncias.com.br/universoamericanas> or phone at 0800 282 25 50.

Situations and complaints reported by the above channels are treated confidentially, with the option of anonymity in all channels. All those involved in reporting violations have their rights to privacy and confidentiality reserved, and any forms of coercion or reprisals are unacceptable.

All reports will be investigated by the Company's Investigation area and classified, following the conclusion of the investigation, as: valid, groundless or inconclusive.

Reports found to be valid will have the appropriate punishments applied.

6. ORGANIZATIONAL STRUCTURE & RESPONSIBILITIES

6.1. Board of Directors

- Evaluating and approving this Policy and reviewing it, whenever necessary;
- Evaluating the effectiveness of this Policy; and
- Ensuring the adoption of corrective and preventive improvements to ensure the effectiveness of this Policy.

6.2. Executive Board

- Ensuring the implementation and application of this Policy and the procedures for preventing and countering money laundering;
- Ensuring that suspected illegal transactions are duly reported to the competent authority, within the regulatory period;
- Monitoring the efficiency and effectiveness of this Policy.

6.3. Internal Audit Area

- Conducting audit to verify compliance with this Policy; and
- Reporting the weaknesses identified to the responsible areas.

6.4. Risk & Internal Control Area

- Ensuring compliance by the business areas with the internal procedures established to prevent and counter money laundering and the financing of terrorism;
- Analyzing the efficiency and effectiveness of procedures and internal controls to prevent and counter money laundering and the financing of terrorism;
- Recommending, when necessary, corrective and/or preventive actions in order to ensure the efficiency and effectiveness of procedures related to preventing and countering money laundering and the financing of terrorism; and
- Clarifying any doubts regarding the content and applications of this Policy.

6.5. Investigation Area

- Receiving and investigating reports related to money laundering and the financing of terrorism made by the Whistleblower Channel and, when necessary, conducting investigations, including those carried out with external support; and
- Reporting the weaknesses identified during the exercise of their investigation activities.

6.6. Marketplace Compliance Area

- Ensuring onboarding, monitoring and relationship with sellers;
- Checking key information and promoting due diligence of sellers; and
- Identifying and evaluating any and all suspicious conduct by sellers, ensuring, upon confirmation, the appropriate treatment (training, warning, suspension or blocking, according to the consequences matrix).

6.7. Payment Method Area

- Collecting, recording, monitoring and reviewing all payment transactions and proposed transactions in order to assess whether there is evidence of involvement in money laundering, terrorist financing and corruption.

6.8. Human Resources

- Checking key information about new and former employees; and
- Ensuring that all employees receive training on the subject covered in this Policy, when necessary.

6.9. Legal Office

- Notifying interested areas when there are any amendments to legal provisions related to money laundering and the financing of terrorism;
- Establishing the necessary criteria for engaging suppliers and service providers, with a focus on preventing and countering money laundering and the financing of terrorism;
- Checking key information about suppliers and service providers;
- Promoting the due diligence of service providers and suppliers; and
- Providing liaison with the competent authorities.

6.10. Employees

- Ensuring and observing compliance with this Policy and, when necessary, notifying Executive Board of situations conflicting with this Policy.

7. MISCELLANEOUS

This Policy comes into force on the date of approval thereof by the Board of Directors.

8. REFERENCE

Regulations governing preventing and counteracting money laundering, terrorist financing, corruption, fraud and violation of sanctions, include, but are not limited to, the following:

- Law No. 9.613 of 1998, which defines the offense of laundering or concealment of assets, rights and values, establishes procedures to be adopted by the entities making up the financial system as a means of preventing the practice of this offense, and, ultimately, establishes the Brazilian Financial Control Council – COAF, administrative agency responsible for receiving, examining and identifying suspicious occurrences and reporting them to the competent authorities.

- Law No. 13.260 of 2016 which governs terrorism and defines the offense of financing terrorism.
- Law No. 12.846 of 2013, which provides for the administrative and civil liability of companies for the practice of acts against the public administration, national or foreign.
- Decree No. 8.420 of 2015, which regulates Law No. 12.846/2013 and provides for the administrative liability of companies for the practice of acts against the public administration.
- CVM Instruction No. 617 of 2020, which provides for the prevention of money laundering and the financing of terrorism within the scope of the securities market.
- SARB Normative No. 011/2013, which establishes guidelines consolidating the best national and international practices for preventing and countering money laundering and the financing of terrorism.